REMARKS

Claims 1-35 are all the claims pending in the application.

Claims 1 and 6 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite.

Claims 1-22, 24-25, 28, 30, 33 and 35 are rejected under 35 U.S.C. 102(e) as being anticipated by Giniger et al. (U.S. Patent No. 6,751,729).

Claims 23, 26-27, 29, 31-32 and 34 are rejected under 35 U.S.C. 103(a) as being anticipated by Giniger et al. (U.S. Patent No. 6,751,729) in view of Rueda et al. (U.S. Patent Application No. 2002/0112076).

The Applicants traverse the rejections and request reconsideration.

Section 112 Rejections

The claims have been amended to overcome their rejections under section 112.

Prior Art Rejections

Rejection of 1-22, 24-25, 28, 30, 33 and 35 based on Giniger

The present invention relates to methods for performing mutual authentication and authorization of a users terminal and an ISP to provide a secure communication between the terminal and a trusted element to the internet via an **untrusted access station.** For example, in the embodiments shown on Figs. 1 and 2, the user terminal 3 is connected to the trusted network element 5 via an untrusted access station 4.

Giniger includes a general teaching on providing secure service communication services over a data network. Further, it teaches establishing a tunneling communication service.

However, the specific issue of accessing an internet in a trusted way between a user terminal via an untrusted access station is not even remotely suggested.

Specifically, the present invention (as recited in claim 1) requires establishing an association between a terminal and an **untrusted access station**. Giniger does not disclose or suggest establishing such an association between a terminal and an **untrusted access station**.

Further, the present invention requires distributing a secure key to a trusted network element for encrypting traffic between the terminal and the trusted network element. Using the encryption, a secure tunnel is established such that the terminal may communicate with the internet via the trusted network element. Specifically, the secure tunnel is required to be established in such a way that the traffic in the secure tunnel is secure from modification by the access station.

Giniger does not disclose (or suggest) establishing an association with an untrusted access station. The Examiner appears to read the untrusted access station on the edge devices 110 (see 9:30-35 of Giniger). However, there is no disclosure (or suggestion) that one or more of these edge devices are untrusted. Even if one of the edge devices 110 are construed to be untrusted, there is no disclosure or suggestion for a terminal to establish association with the edge device 110 and then subsequently distributing a session key to a second edge device for establishing a secure tunnel between the terminal and this second edge device. The passages cited by the Examiner (15:19-22) merely suggests establishing tunnels between edge nodes.

The inventive method requires a sequence of steps. The Examiner appears to misconstrue aspects of the teachings of Giniger to read on some of the steps. However, the

entire sequence of steps in the present invention (as recited in claim 1) is not suggested by Giniger. Claim 1 is not anticipated by Giniger because it does not disclose all the steps in the proper sequence.

Claims 4, 5 and 6 include features analogous to claim 1. Therefore, the above arguments are analogously valid.

Further, claim 4 requires that the packets flowing between the terminal and the trusted network element be transmitted via the untrusted access station. As noted above, Giniger does not disclose the concept of a trusted network element and an untrusted access station. Furthermore, it does not disclose (or suggest) that the packets be transmitted between the terminal and the trusted network element via the untrusted access station. In fact, Giniger merely suggests direct exchange of packets between two edge devices and not sending them via a third edge device.

Claim 5 requires the secure tunnel to enable the ISP to dynamically obtain control of resources in the untrusted access station. There is no disclosure (or suggestion) for a secure tunnel between the edge devices of Giniger to be able to control the resources of another end node.

Claim 6 includes limitation analogous to the one discussed above in relation to claim 5.

Claims 2, 3, 7-21, 24-25, 28, 30 and 30 are dependant on claims 1 and 6, respectively. Therefore, they are patentable for the same reasons.

Claim 35 recites a computer program product and includes limitations analogous to the ones discussed above. Therefore, it is patentable at least for analogous reasons.

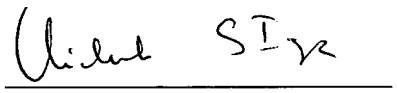
Rejection of claims 23, 26-27, 29, 31-32 and 34 base on Giniger and Rueda

The above claims are dependant on claim 6, and therefore, are allowable for at least the same reasons. Further, Rueda does not overcome the deficiencies noted above in the teachings of Giniger.

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,



Chid S. Iyer
Registration No. 43,355

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: June 21, 2005